Western Connecticut
COUNCIL OF GOVERNMENTS

February 25, 2024

Esteemed Chairs Maroney and Lemar,
Members of the General Law Committee:

The Western Connecticut Council of Governments (WestCOG) appreciates the opportunity to comment on Committee Bill 2, *An Act Concerning Artificial Intelligence.* This bill will help to ensure artificial intelligence (AI) is deployed responsibly. We recognize the bill's focus on bias prevention, transparency, and fairness, particularly in areas such as employment, finance, healthcare, housing, and government services. As AI technology advances, new risks may emerge that warrant additional legislative attention. WestCOG has identified the corruption of public trust and financial instability as threats that your Committee may wish to address:

I. PROTECTING PUBLIC TRUST AND PREVENTING AI-DRIVEN MANIPULATION

AI's capacity to generate persuasive and large-scale content poses significant risks to public discourse and governance. Unlike traditional misinformation tactics, AI can rapidly generate, modify, and interact with users in real time, creating an evolving and automated system of deception that is difficult to detect or counteract. These capabilities make AI a powerful tool for distorting public opinion, misleading consumers, and overwhelming democratic institutions.

Case Studies Highlighting the Risks:

- Election Interference – In 2016, the Russian government conducted a multifaceted campaign to influence the U.S. presidential election, employing tactics such as hacking and leaking sensitive information, funding deceptive advertisements, and deploying fake social media accounts to disseminate divisive narratives. While these efforts were not AI-driven, they underscore the vulnerability of democratic processes to coordinated disinformation. The advent of AI technologies capable of creating highly realistic synthetic content, such as deepfakes and automated bot networks, could exponentially amplify these threats, making it increasingly challenging to discern authentic information from manipulation.

- Net Neutrality Comment Fraud – During the Federal Communications Commission's (FCC) 2017 public comment period on net neutrality, investigations revealed that major broadband companies financed a campaign that resulted in the submission of over 8.5 million fake comments opposing net neutrality. These comments impersonated real individuals without their consent, undermining the integrity of the public feedback process. This deception was executed without AI assistance, allowing investigators to identify the fraudulent submissions. The integration of AI could make future detection efforts significantly more difficult.

- The Grok Incident – The AI assistant Grok, developed by xAI and integrated into the platform X (formerly Twitter), was initially designed to provide objective information, including highlighting instances where its owner, Elon Musk, had disseminated misinformation. However, subsequent reprogramming altered Grok's responses to omit negative references to Musk,

demonstrating how AI systems can be intentionally modified to suppress or manipulate information for personal or political gain.

Policy Responses

To address these risks, your Committee may wish to consider policies such as the following:

- Conflict of Interest Protections in State Contracting – Prohibit the allocation of state funds or subsidies to entities whose executives hold prominent positions in federal or state government, preventing potential conflicts of interest and undue influence over AI-related policies and procurement.
- Verification of Human Submissions in Public Processes – Require government agencies to implement CAPTCHA-like verification mechanisms for public comment submissions, ensuring that responses originate from actual individuals rather than AI-generated spam. Such systems should be designed to prevent bot interference while remaining accessible to all users.
- Transparency in AI Model Modifications – Mandate that organizations disclose significant changes to AI systems that influence public-facing content, ensuring stakeholders are informed about alterations that could impact information dissemination.
- Standards for AI Content Moderation – Encourage the development and enforcement of robust policies by online platforms to identify and manage AI-generated misinformation effectively.
- Digital Literacy and Public Awareness Initiatives – Invest in educational programs that equip residents with the skills to critically evaluate AI-generated content, fostering resilience against misinformation and manipulation.

II. ENSURING FAIRNESS AND STABILITY IN AI-DRIVEN FINANCIAL MARKETS

AI is increasingly driving algorithmic trading, investment decisions, and financial risk assessments across both conventional markets and cryptocurrency ecosystems. While AI offers efficiencies and predictive capabilities, it also introduces new forms of systemic risk, market distortion, and financial manipulation. Without appropriate safeguards, AI-driven financial systems could exacerbate volatility, facilitate fraud, and create enforcement challenges across both regulated and decentralized markets. The risks associated with AI in financial markets and cryptocurrencies can be grouped into three major categories: market instability, AI-enabled financial manipulation, and consumer and investor exploitation.

Market Instability and Systemic Risk

AI-driven trading algorithms can react to market signals in unison, amplifying volatility and triggering cascading failures. This phenomenon, known as algorithmic convergence, occurs when multiple AI systems make similar trading decisions based on shared data patterns. Because AI models are trained on past market behavior, they may reinforce trends rather than counteract them, creating self-perpetuating cycles of instability.

In addition, unintentional collusion can emerge when independent AI systems develop similar trading strategies without direct coordination. While not explicitly illegal, this behavior can reduce

market competition and create price distortions that harm investors. AI systems operating at high speeds may also engage in race conditions, where multiple algorithms compete to execute trades within fractions of a second. These conditions can lead to unexpected liquidity shortages, price anomalies, and rapid market crashes—events that are difficult to control once they begin.

These risks are not confined to traditional markets. Cryptocurrency trading is particularly susceptible to AI-driven volatility due to its lower liquidity, lack of centralized oversight, and susceptibility to automated trading bots. Unlike stock exchanges with circuit breakers to halt extreme fluctuations, cryptocurrency markets operate continuously and lack safeguards against AI-induced flash crashes or liquidity shortages.

AI-Enabled Market and Financial Manipulation

AI provides bad actors with new tools to manipulate financial markets and cryptocurrency ecosystems at a scale and speed far beyond traditional methods. AI-powered trading systems can autonomously generate and amplify disinformation, execute high-speed spoofing strategies that create false market signals, and manipulate financial sentiment by analyzing and selectively promoting narratives across news and social media platforms.

One example of how disinformation can destabilize markets occurred on April 23, 2013, when a false tweet from the Associated Press's hacked Twitter account reported explosions at the White House. Within minutes, automated trading systems reacted, causing the Dow Jones Industrial Average to drop 143 points before the misinformation was corrected. While this incident was not AI-driven, it highlights the potential for AI-powered networks to intentionally flood the market with false signals, creating far more severe and sustained disruptions.

AI-powered fraud extends beyond regulated markets into decentralized finance (DeFi) and cryptocurrency trading. AI can be used to manipulate token prices through pump-and-dump schemes, where automated bots artificially inflate cryptocurrency values before large, coordinated sell-offs occur, deceiving investors. Front-running, where AI detects pending transactions and executes trades milliseconds before them to extract profits, is already a known issue in DeFi. AI-driven sentiment analysis can also be used to artificially boost or suppress confidence in specific tokens, influencing prices in ways that evade traditional regulatory oversight.

Furthermore, AI enables highly sophisticated financial fraud, including deepfake-based scams. AI-generated personas and voice-cloned recordings can impersonate trusted figures to persuade victims into fraudulent cryptocurrency investments. "Pig butchering" scams—where victims are tricked into believing they are engaging in lucrative trading opportunities before their assets are drained—have become increasingly AI-enhanced, making them harder to detect.

AI and the Consumer/Investor

AI-driven financial tools have democratized investing, but they have also introduced new risks for consumers and retail investors in both traditional and digital markets.

The rise of commission-free trading platforms, such as Robinhood, has made financial markets more accessible, yet it has also exposed retail investors to AI-driven manipulation. AI-powered trading models can anticipate, exploit, or even trigger retail trading trends, allowing certain

interests to front-run small investors. For instance, AI can scan online financial discussions, predict which stocks or tokens are likely to become "meme assets," and capitalize on market movements before the average investor has time to react.

In the cryptocurrency space, AI-enhanced fraud extends beyond market manipulation to exploit vulnerabilities in digital asset storage and transactions. AI can identify weaknesses in smart contracts, automate exploitative attacks on DeFi protocols, and circumvent traditional security measures by launching adaptive cyberattacks that evolve in real-time. Because blockchain transactions are irreversible, once assets are lost to AI-powered fraud, they cannot be recovered.

AI-generated financial recommendations, automated portfolio management tools, and trading bots introduce additional risks if biased, misleading, or deliberately programmed to serve specific financial interests. Consumers may unknowingly follow AI-generated investment strategies designed to benefit centralized exchanges, hedge funds, or large stakeholders at their expense.

Policy Responses
To address these risks, your Committee may wish to consider policies such as the following:

- State-Level Legal Recourse for AI-Driven Fraud – Allow state financial regulators to pursue legal action against AI-driven entities engaging in deceptive trading practices, including fraudulent cryptocurrency investment schemes and AI-enhanced cybercrime.
- AI Market Oversight and Transparency – Require AI-driven trading firms, including cryptocurrency exchanges and DeFi platforms, to disclose key aspects of their algorithms and decision-making processes to financial regulators, ensuring visibility into potential risks posed by autonomous trading.
- Mitigation of AI-Induced Systemic Risk – Develop new risk management frameworks that account for algorithmic convergence, unintentional collusion, and AI-driven volatility, ensuring that market safeguards are adapted for the speed and scale of AI trading.
- Protection Against AI-Enabled Financial Manipulation – Strengthen enforcement mechanisms against AI-driven spoofing, disinformation campaigns, pump-and-dump schemes, and AI-powered front-running in both traditional and digital markets.
- Regulatory Protections for Retail Investors and Crypto Users – Establish safeguards ensuring that AI-driven trading does not unfairly exploit retail investors or cryptocurrency users, including oversight of AI-generated financial recommendations, DeFi exploit prevention, and enhanced consumer protection measures.

III. CONCLUSION

Artificial intelligence is rapidly transforming both public discourse and financial markets, introducing profound risks that demand proactive governance. In public trust and governance, AI-driven misinformation, deepfake content, and the manipulation of public feedback processes threaten to erode democratic integrity and distort decision-making. The ability of AI to generate and amplify misleading narratives on a massive scale underscores the need for stronger

transparency, verification mechanisms, and conflict of interest protections to safeguard public institutions.

In financial markets and cryptocurrencies, AI creates new risks of systemic instability, market manipulation, and investor exploitation that require updated safeguards. The increasing reliance on AI in high-frequency trading, sentiment-driven investing, and decentralized finance (DeFi) has introduced vulnerabilities that traditional regulations were not designed to address. Without intervention, AI-driven market distortions could undermine financial stability, disadvantage retail investors, and facilitate fraud on an unprecedented scale.

Your Committee has the opportunity through bill 2, or another vehicle, to help Connecticut proactively address AI-related threats across multiple sectors while ensuring innovation is balanced with strong consumer, investor, and democratic protections.

I appreciate the Committee's leadership on this critical issue and thank you for your consideration. Please do not hesitate to contact me should you have questions or require additional information.

Francis R. Pickering
Executive Director